ABSTRACT OF THE DISCLOSURE

A system and a method to reduce a search space to determine viable cellular automata based random number generators (CA-based RNGs) are presented. A CA-based RNG is where an output of each cell of the CA at time t is dependent on inputs from any cells of the CA (including perhaps itself) at time t – 1. The connections (or inputs) are selected to produce high entropy such that the RNG passes a standard suite of random number of tests, such as the DIEHARD suite. As the number of inputs grow (corresponding to the neighborhood size), the number of truth tables grows dramatically. By reducing the search space of viable CA-based RNGs, high quality random number generators with higher neighborhood sizes may be found.